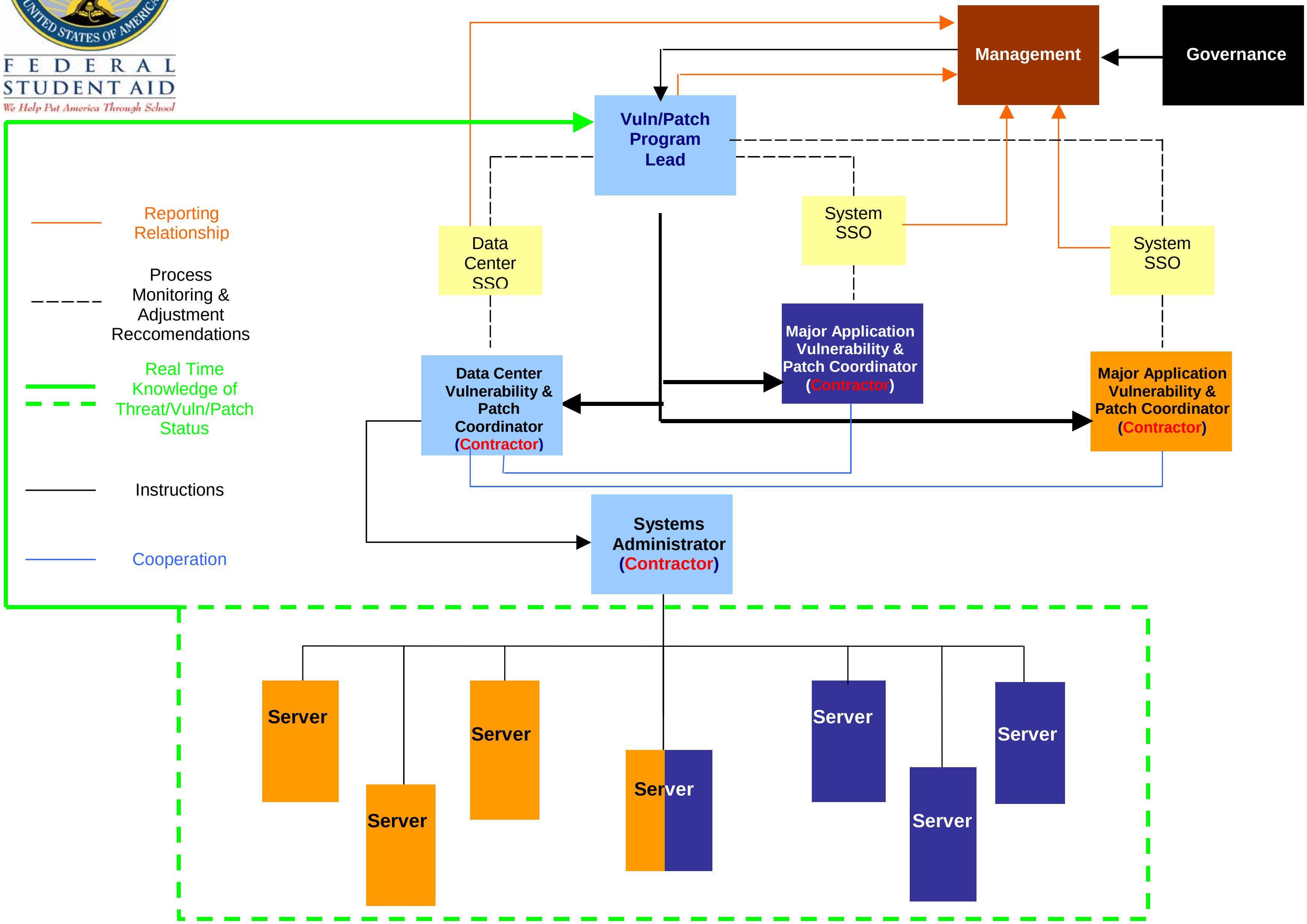
FEDERAL STUDENT AID

We Help Put America Through School

FSA Security Vulnerability/Patch Management

Real-Time Discovery, Corrective Action Instruction and Procedure Dissemination, Monitoring, Reporting, & Accountability



Management

Governance

Vuln/Patch Program Lead

Data Center SSO

System SSO

System SSO

Major Application Vulnerability & Patch Coordinator (Contractor)

Data Center Vulnerability & Patch Coordinator (Contractor)

Major Application Vulnerability & Patch Coordinator (Contractor)

Systems Administrator (Contractor)

Server

Server

Server

Server

Server

Server

Server

Reporting Relationship

Process Monitoring & Adjustment Reccomendations

Real Time Knowledge of Threat/Vuln/Patch Status

Instructions

Cooperation

FSA Security Vulnerability/Patch Management

Real-Time Discovery, Corrective Action Instruction and Procedure Dissemination, Monitoring, Reporting, & Accountability

Overview

In order to competently manage FSA's security posture, BearingPoint recommends that the organization systematically deploy a series of commercially available tools to enable and enforce detection and remediation of enterprise wide vulnerabilities.

These tools are part of a design that accommodates the business and technical requirements of owners and operators of major applications and data centers while providing senior security management with a centralized means of knowing real-time threat exposure, disseminating remediation advice, and tracking and ensuring results.

Results are ensured using proven, automated, accountability strategies, methods, and techniques that are integrated into the design. Details of the accountability component are part of a forthcoming document.

The purpose of this document is to convey the framework of governance, information flow, and relationships of participating personnel - and to do that in the context of the first tool to deploy – a security patch management tool.

Governance

FSA Vulnerability and Security Patch Management Policy

A security patch management policy issued by senior FSA management will mandate that senior security management know the state of exposure relative to unpatched software in as close to real-time as possible.

The policy will require that senior security management institute and maintain a program that ensures efficient and effective patch management. The policy will require the institution of an efficient and effective means of disseminating all advisory and remediation instructions and that automation of workflow and accountability be put into place to ensure results.

The policy will not delineate time or testing requirements. It will define roles and responsibilities. Vulnerability/Patch severity conditions will be defined and dictate accountability scope not patch deployment scope.

For example, critical severity will set the automated predefined wheels in motion to define relevant system impact. And so on.

FSA Vulnerability and Security Patch Management Guidance

This document provides assistance in decision making relative to patch deployment and major application business operational criticality.

FSA Vulnerability and Security Patch Management Procedures

This is a living document that will provide recommendations for actions associated with testing and deployment of patches based on industry best practices.

FSA Security Vulnerability/Patch Management

Real-Time Discovery, Corrective Action Instruction and Procedure Dissemination, Monitoring, Reporting, & Accountability

Framework for Information Flow and Participant Relationships

This framework is version 1.3. The tool required to start the program and facilitate the information flow consists of comprehensive discovery, monitoring, and remediation capabilities using agent technology. The agent technology is open to allow for integration and interoperability with future risk mitigation tools.

Using this design and toolset, a real-time self-auditing and remediation planning & deployment program will ensure compliance with federal regulations, reduce the depth and breadth of audits and contribute greatly to successful certification and accreditation of all FSA systems. Most important, FSA's information security posture becomes greatly enhanced and imminently flexible to the security requirements of future IT systems and regulations.

Management

Security Management is enabled, guided, and held accountable by the security patch management policy to ensure that the security vulnerability and patch management program is improving the organizations security posture.

Security Management uses the toolset to:

- Monitor Exposure
- Define and fine-tune the rules for accountability, workflow, monitoring, and reporting.
- Monitor the program
- Enforce the policy

Vulnerability/Patch Program Lead

This individual administers the console to monitor and report daily on the state of security patch management in the enterprise. Responsibilities include:

- Ensuring the security of all media containing vulnerability information
- Monitoring and reporting of accountability deficiencies to security management
- Accommodating management's report requests
- Disseminating instructions and advisories and/or ensuring their automated delivery and acceptance in a timely manner and in accordance with policy defined severity conditions
- Aggregate process adjustment input from constituency for delivery to management
- Maintain current level of training on tools
- New agent deployment when necessary

SSO

Data Center and Major Application System Security Officers are responsible for monitoring the process from Program Lead through to their contractor coordinator to identify process weakness and act as a bridge for input and resolution of issues between management and the data center or major application vulnerability/patch coordinator. Other responsibilities include:

- Ongoing assessment of security posture for respective domain
- Monitor external advisory resources to ensure consistency and currency of program
- Other

Major Application Coordinator

In most cases, if not all, this individual is a contractor and responsible for proper operation of the major application and its components. At FSA, this individual already coordinates with the data center contractor to do system maintenance.

For vulnerability and patch management, the same applies with the additional responsibility of responding to workflow and accountability demands of this program. Some of these demands are:

- Major contributor to impact assessment workflow
- Aids in determining patch deployment schedule
- Reports any performance issues or breaks associated with remediation
- Other

Data Center Coordinator

The data center security vulnerability/patch coordinator is a contractor who will respond to the instructions of the program lead. The contractor must perform according to the final deployment instructions. Means or manner of deployment are left to the contractor, however, a very efficient means of deployment will be inherently available with this tool.

As mentioned, contractor can use any means he/she sees fit to deploy the patches – using existing/preferred methods, tools, etc., - but must remain in compliance with the instructions of the Program Lead. Usually, this will mean timely reporting on the process of any testing, staging, deployment of patches and/or any alternate or accompanying remediation. A working paper for instructions is forthcoming.

Systems Administrator

The systems administrator takes action based on the instruction of the data center coordinator who is usually an employee of same contractor. This individual performs actual deployment by physically testing and installing patches or performing alternate and/or accompanying remediation measures.

FSA Security Vulnerability/Patch Management

Real-Time Discovery, Corrective Action Instruction and Procedure Dissemination, Monitoring, Reporting, & Accountability

Notes:

Block Colors On the Flow Chart

⬛ Policy, Guidance, Procedures

🟫 Security Management

🟦 Program Lead, Data Center Vulnerability/Patch Coordinator, and Systems Administrator are colored the same light blue to show the direct pipeline of physical remediation instruction

🟦🟧 Major Applications and associated personnel. Because more than one major applications are often hosted in the same data center, they may share resources. This is depicted in the navy and orange server

🟨 System Security Officers